2002-518726
2002.6.25

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
(Related application)
This application asserts the priority based on the U.S. temporary application number 60 of application / 995 on June 19, 1998. [089 and 995]
[0002]
(Technical field of invention)
This invention relates to filtering of the information transmitted between a proxy server, the client process using a plug-in filter, and a web server in more detail about filtering of the information transmitted between a client process and a server process.
[0003]
(Background technique of invention)
By the rapid spread of the Internet, accessible amount of information increased from the company or the consumer remarkably. Managing an informational inflow is increasing significance gradually. It is because the information which a user does not expect not to desire to be opened to the others on the Internet, or to be sent by the others is included in information. By connecting a computer or a network to the Internet, a user can retrieve, access and download all types of information from the safe information of the information of a government agency to the information about amusement. Since most regulations on the Internet were not performed, access to all types of information increased dramatically. However, a user may need to filter to the information taken out from a network. For example, it is necessary to make it, as for a company or a government agency, neither security information nor extra sensitive information flow out of the domain of oneselves, such as a local network. Moreover, the information received from the Internet cannot be operated in the format by the side of reception. For example, the property of the display resolution of the document received from the Internet may differ from the property which the user by the side of the reception of a document supports.
[0004]
In order to cope with an above-mentioned problem, the system which prevents a certain information's flowing into a domain, or flowing out of a domain has been developed. As for informational filtering, what can be performed is complicated, and such a system is not easy to fit a specific company. Generally, the system which filters information cannot change after that the point what kind of information to remove how, once it is created by the software-development person, and for that purpose, the software-development person completely needed to re-create the filtering system newly. The needs which information the problem in this approach filters how are in the point of in almost all cases being specification and changing to each company and user. It is not realistic to reconstruct a system by the software-development person, whenever a user is going to filter different contents. Furthermore, the system which corrects at present the data which were not able to be operated in a user environment in the phase received first so that it may be operational does not exist.
[0005]

The function for taking an interface with a computer is simplified by using the Internet, especially World Wide Web ("web"). The architecture of a web shall follow the conventional client-server model. Among the roles of a computer, in general, a role of a claimant (client) of data, or since a role of a feeder (server) of data is expressed in general, the vocabulary a "client" and a "server" is used. In a web environment, a web browser is in a client side and the "web document" to which the specific format was performed is in the Internet web server side. A web client and a web server usually communicate mutually using the protocol called "hypertext transferred protocol" (HTTP).
[0006]
At the time of activation, a browser opens connection with a server and performs the demand to a document. A server usually hands over the demanded document in the format encoded in the standard "hypertext markup language" (HTML) format. Connection is closed after handing over a document. A browser displays a document and performs the function specified by the displayed document. Therefore, improvement in an informational filtering technique is desired.
[0007]
(Outline of invention)
The approach concerning this invention, a system, and a manufacture are conquered by having the proxy server which possesses a plug-in filter for the fault which the existing information system for filtering information between a client process and a server process holds. According to the proxy server possessing a plug-in filter, it can change easily which information is filtered how. In addition, it becomes possible by using a plug-in filter not only correction like the informational exenteration but to correct an informational property so that it may correspond to the environment of a client process or a server process.
[0008]
In the approach of filtering the information from the 1st process to the 2nd process as according to the 1st description of this invention it embodies here and the outline is explained this approach By correcting said information based on the process which receives said information from said 1st process, the process which chooses the filter for applying to the information received according to said 1st process, and the instruction included in said filter Let it be a summary to have the process which applies said filter to said information, and the process which transmits said corrected information to said 2nd process. Said 1st process may be a client process, said information may be a demand and said 2nd process may be a server process. Said information included in said demand may be security data. Or said 1st process may be a server process, said 2nd process may be a client process, said information may be a response, and said corrected information may be the corrected response. Furthermore, said filtered response may be stored in cache memory. The aforementioned process which chooses the filter applied to said information is Uniform. Resource When said defined URL agrees with the process which defines Locator (URL) and a corresponding filter, and the process which takes out URL from said information in said taken-out URL, you may have the process which chooses said filter corresponding to said defined URL for applying to said information.
[0009]
In the approach of filtering information using a proxy server as according to other descriptions of this invention it embodies here and the outline is explained furthermore, this approach The process which receives a demand from a client process, and the process which applies a forward direction filter to said demand, The process which transmits said filtered demand to a server process, Let it be a summary to have the process which receives the response about said filtered demand from said server process, the process which applies a hard flow filter to said response, and the process which transmits said filtered response to said client. Said 2nd process may be a web server and the aforementioned process which applies said forward direction filter in this case may also include the process which defines URL and a corresponding filter, and the process which filters said demand using said corresponding filter when said defined URL is contained in said demand. Moreover, the aforementioned process which applies said hard flow filter when said 2nd process is a web server may also include the process which defines URL and a corresponding filter, and the process which filters said demand using said corresponding filter

when said defined URL is contained in said response. Said filtered response may be stored in cache memory.

[0010]

In the approach of adding a filter to a proxy server as according to other descriptions of this invention it embodies here and the outline is explained furthermore, this approach The process which creates said proxy server which operates so that a filter may be received, Having the process which creates the filter possessing a filter regulation and a filter servlet, and the process which adds said filter to said proxy server, said proxy server makes it a summary to operate so that information may be corrected using said added filter.

Two or more filters may be added to said proxy server.

[0011]

(Detailed description)

The accompanying drawing which is used for this specification and constitutes some of these specifications illustrates operation of this invention, and explains the advantage and principle of this invention with detailed explanation of this invention.

[0012]

Hereafter, the gestalt of 1 operation of this invention shown in an accompanying drawing is explained to a detail. In addition, in a drawing and the following explanation, it referred to using the same sign about the same or similar part.

[0013]

(Installation) The system and approach concerning this invention perform forward direction filtering and hard flow filtering using a plug-in filter to the information transmitted between a client process and a server process. A proxy server supervises the demand and response which are transmitted among both while taking the interface of a server process and a client process. The system and approach which are explained in this operation gestalt can enable him for a user to create a filter and to define this as a proxy server, and, therefore, a user can fit to his needs which information is filtered how. These plug-in filters correct the information between a client process and a server process by a certain fixed approach. The correction on the basis of the contents of removing security information is sufficient as this correction, or modification which makes information operational for the information sent from a server process also in a client process, and gives compatibility, such as modification of for example, a display resolution property, is sufficient as it.

[0014]

Furthermore, a proxy server interfaces with a client process and a server process at a detail. A filter is created and plug-in is carried out to a proxy server. A filter has a filter regulation and a filter servlet. A filter regulation specifies the information which should be removed. For example, Uniform of a demand Resource All the information required of URL by which Locator (URL) could be defined as a filter regulation, therefore the client process was defined will have the filter applied. When a filter servlet is performed, it is an actual instruction which corrects the information included in a demand or a response. Therefore, once the indicator which expresses the purport which requires filtering when the above-mentioned example is described is given to a demand, by comparing with defined URL, the filter servlet corresponding to a filter regulation will be performed, and the information included in a demand will be corrected by the fixed approach.

[0015]

The approach and system concerning this invention support addition of two or more plug-in filters again. By adding a filter, in case a user corrects which information how, he can change a large number. Furthermore, the approach and system to apply can also be constituted so that the management task in connection with the demand between a client process and a server process and transmission of a response may be performed. Moreover, storing in cache memory can also be performed and, thereby, a large number to the same information can be accessed promptly. In case storing in cache memory is performed, in order to abolish the need of applying a filter to the response received from the server process again, it is desirable to store the filtered response in cache memory.

[0016]
Drawing 1 shows further the example of the client/server system which interconnected through the network 100 in the detail. In this example, the remote server system 122 interconnects to the client system 120 through a network 100. The client system 120 contains the usual component. For example, the bus 126 which connects a processor 124, memory 125 (for example, RAM), and a processor 124 and memory 125, the large capacity storage 127 (for example, a magnetic hard disk or an optical storage disk) connected to a processor 124 and memory 125 through I/O-hardware-control equipment 128, and a network interface 129 like the usual modem are included.
[0017]
The server system 122 also contains the usual component. For example, the bus 136 which connects a processor 134, memory 135 (for example, RAM), and a processor 134 and memory 135, the large capacity storage 137 (for example, a magnetic disk or an optical disk) connected to a processor 134 and memory 135 through I/O-hardware-control equipment 138, and a network interface 139 like the usual modem are included. It will be recognized from the following publication that this invention may be mounted in each of the large capacity storage 127 and 137 on a client/server system or each computer-readable medium [like] of memory 125 and 135 in the software stored as an instruction which can be executed.
[0018]
Although the network shown in drawing 1 shows the network as an example, it will be understood by this contractor that you may be what kind of topology containing the Internet, the private network, and internal computer structure which enable the module in various computer systems or a single computer structure to exchange information.
[0019]
Drawing 2 shows the suitable data processing system for operation of the approach and system concerning this invention. Data processing system 200 has intranet 202 and the Internet 204. Intranet 202 expresses the network of an organization and contains a computer 206, a computer 208, and a fire wall 214. A fire wall 214 supervises both the turning-inward traffic to intranet 202, and the extroversion traffic to the Internet 204. The computer 206 and the computer 208 both have many components, and memory 215 and 217, secondary storages 219 and 221, at least one I/O devices 223 and 225, and processors 227 and 229 correspond to this component. The Internet 204 contains computers 206 and 208 and the computers 210 and 212 which have the same component. Although described with intranet 202 and the Internet 204 having only two computers, this contractor will also understand that these networks may contain further many computers. In addition, this contractor will understand that the approach and system concerning this invention can be used by other Local Area Networks or Wide Area Networks. Moreover, computers 206, 208, 210, and 212 may also contain the further component or further different component.
[0020]
The fire wall 214 contains memory 224, the processor 226, and the secondary storage 240. According to the approach and system concerning this invention, memory 224 has the proxy server 228 and the proxy server 230. Proxy servers 228 and 230 have filters 232 and 234, respectively. A proxy server 228 performs "forward direction filtering" using a filter 232. "Forward direction filtering" expresses filtering performed to the response of these demands only to the demand by which it is sent to the Internet 204 while a proxy server occurs from the intranet 202 interior. For example, the client program 216 of a computer 206 tends to access the server program 220 of a computer 210. In this case, a filter 232 expresses not only all the parts of ** which should be blocked, and a response but the extroversion demand which can pass a fire wall and can flow and a turning-inward response. That is, filtering performed by the approach and system concerning this invention includes blocking blocking that a part of website is accessed or that the whole website is accessed.
[0021]

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2002－518726
（P2002－518726A）
(43)公表日　平成14年６月25日(2002.6.25)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
Ｇ０６Ｆ　12/00	５４６	Ｇ０６Ｆ　12/00	５４６Ｒ　５Ｂ０８２
13/00	３５１	13/00	３５１Ｚ　５Ｂ０８９

審査請求　未請求　予備審査請求　有　（全 33 頁）

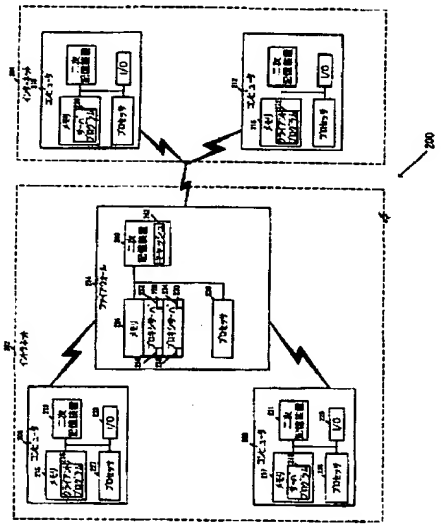
(21)出願番号　特願2000－555143(P2000－555143)
(86)（22)出願日　平成11年６月18日(1999.6.18)
(85)翻訳文提出日　平成12年12月19日(2000.12.19)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／１３８７６
(87)国際公開番号　ＷＯ９９／６６３８５
(87)国際公開日　平成11年12月23日(1999.12.23)
(31)優先権主張番号　６０／０８９，９９５
(32)優先日　平成10年６月19日(1998.6.19)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＪＰ

(71)出願人　サンマイクロシステムズ　インコーポレーテッド
アメリカ合衆国、94043　カリフォルニア州、マウンテン　ビュー、ガルシア　アヴェニュー　2550
(72)発明者　ナジャール　ビベック
アメリカ合衆国、94806　カリフォルニア州、サニーベール、　エスカロン　アベニュー　1055
(74)代理人　弁理士　上野　登

最終頁に続く

(54)【発明の名称】　プラグインフィルタを用いた拡張性の高いプロキシサーバ

(57)【要約】
【課題】フィルタリングする内容及び方法に関しユーザが容易に変更を行えるように、フィルタリング技術を向上させること。
【解決手段】本発明に係るプロキシサーバは、プラグインフィルタを具備する。本発明に係る情報のフィルタリングを行う方法は、プロキシサーバ（２２８）によりクライアント（２１０）からの要求を受け取る工程を含む。前記プロキシサーバ（２２８）は、要求に含まれる、サーバプロセス（２０８）のＵＲＬをシステムに対して予め定義されたフィルタ規則と比較する。前記ＵＲＬが前記フィルタ規則の１つを満たせば、対応するフィルタサーブレットを用いて情報のフィルタリングを行う。フィルタリングされた要求は、サーバプロセス（２０８）から情報を取り出すのに用いられる。クライアントプロセス（２１０）へのサーバプロセス（２０８）からの応答に対しても同様にフィルタリング処理が行われる。



【特許請求の範囲】

【請求項１】　第１のプロセスから第２のプロセスへの情報をフィルタリングする方法において、該方法は、

前記第１のプロセスから前記情報を受け取る工程と、

前記第１のプロセスにより受け取った情報に適用するためのフィルタを選択する工程と、

前記フィルタに含まれる命令に基づき前記情報を修正することにより、前記フィルタを前記情報に適用する工程と、

前記修正された情報を前記第２のプロセスに送信する工程とを備える。

【請求項２】　請求項１に記載の方法において、前記第１のプロセスはクライアントプロセスであり、前記情報は要求であり、前記第２のプロセスはサーバプロセスである。

【請求項３】　請求項２に記載の方法において、前記情報を修正する前記の工程は、前記情報からセキュリティデータを取り除く工程を含む。

【請求項４】　請求項１に記載の方法において、前記第１のプロセスはサーバプロセスであり、前記第２のプロセスはクライアントプロセスであり、前記情報は応答であり、前記修正された情報は修正された応答である。

【請求項５】　請求項４に記載の方法であって、該方法は、更に、前記修正された応答をキャッシュメモリに格納する工程を備える。

【請求項６】　請求項１に記載の方法において、前記第２のプロセスはウェブサーバであり、前記情報に適用するフィルタを選択する前記の工程は、

第１のＵｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）と対応するフィルタとを定義する工程と、

前記情報から第２のＵＲＬを取り出す工程と、

前記第１のＵＲＬが前記第２のＵＲＬに合致した場合に、前記情報に適用するための、前記定義されたＵＲＬに対応する前記フィルタを選択する工程とを備える。

【請求項７】　請求項１に記載の方法であって、該方法は、更に、プラグインフィルタを追加する工程を含む。

【請求項８】　請求項に７に記載の方法において、前記情報に適用される前記フィルタは前記プラグインフィルタである。

【請求項９】　第１のプロセスから第２のプロセスへの情報をプロキシサーバによりフィルタリングする方法において、該方法は、

Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）をフィルタ規則として定義し、対応するフィルタサーブレットを定義する工程と、

前記第１のプロセスから前記情報を受け取る工程とを備え、前記情報はＵＲＬを含み、前記方法は、更に、

前記情報に含まれる前記ＵＲＬが、前記フィルタ規則に含まれる前記ＵＲＬに合致する場合に、前記情報に適用するための、前記定義されたＵＲＬに対応する前記フィルタサーブレットを選択する工程と、

前記フィルタサーブレットに含まれる命令に基づき前記情報を修正することにより、前記フィルタサーブレットを前記情報に適用する工程と、

前記修正された情報を前記第２のプロセスに送信する工程とを備える。

【請求項１０】　請求項９に記載の方法において、前記第１のプロセスはクライアントプロセスであり、前記情報は要求であり、前記第２のプロセスはサーバプロセスである。

【請求項１１】　請求項１０に記載の法において、前記情報を修正する前記の工程は、前記情報からセキュリティデータを取り除く工程を含む。

【請求項１２】　請求項９に記載の方法において、前記第１のプロセスはサーバプロセスであり、前記第２のプロセスはクライアントプロセスであり、前記情報は応答であり、前記修正された情報は修正された応答である。

【請求項１３】　請求項１２に記載の方法であって、該方法は、更に、前記修正された応答をキャッシュメモリに格納する工程を備える。

【請求項１４】　請求項１に記載の方法であって、該方法は、更に、前記プロキシサーバに対し他のフィルタ規則と他のフィルタサーブレットを定義することにより、プラグインフィルタを追加する工程を含む。

【請求項１５】　プロキシサーバを使って情報をフィルタリングする方法において、該方法は、

クライアントプロセスから要求を受け取る工程と、

前記要求に順方向フィルタを適用する工程と、

前記フィルタリングされた要求をサーバプロセスに送信する工程と、

前記フィルタリングされた要求に関する応答を前記サーバプロセスから受け取る工程と、

前記応答に逆方向フィルタを適用する工程と、

前記フィルタリングされた応答を前記クライアントに送信する工程とを備える。

【請求項１６】　請求項１５に記載の方法において、前記第２のプロセスはウェブサーバであり、前記順方向フィルタを適用する前記の工程は、

Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）と対応するフィルタとを定義する工程と、

前記定義されたＵＲＬが前記要求に含まれている場合に、前記対応するフィルタを使って前記要求をフィルタリングする工程とを含む。

【請求項１７】　請求項１５に記載の方法において、前記第２のプロセスはウェブサーバであり、前記逆方向フィルタを適用する前記の工程は、

Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）と対応するフィルタとを定義する工程と、

前記定義されたＵＲＬが前記応答に含まれている場合に、前記対応するフィルタを使って前記要求をフィルタリングする工程とを含む。

【請求項１８】　請求項１５に記載の方法であって、該方法は、更に、前記修正された応答をキャッシュメモリに格納する工程を備える。

【請求項１９】　請求項１５に記載の方法であって、該方法は、更に、プラグインフィルタを追加する工程を含む。

【請求項２０】　請求項１９に記載の方法において、前記情報に適用される前記フィルタは前記プラグインフィルタである。

【請求項２１】　プロキシサーバにフィルタを追加する方法において、該方法は、

フィルタを受け取るように動作する前記プロキシサーバを作成する工程と、

フィルタ規則とフィルタサーブレットとを具備するフィルタを作成する工程と、

前記フィルタを前記プロキシサーバに追加する工程とを備え、前記プロキシサーバは、前記追加されたフィルタを使って情報を修正するように動作する。

【請求項２２】　請求項２１に記載の方法において、前記フィルタ規則は、Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）を含み、前記フィルタサーブレットは、実行されると前記情報を修正する命令を含む。

【請求項２３】　請求項２１に記載の方法であって、該方法は、更に、複数のフィルタを前記プロキシサーバに追加する工程を備える。

【請求項２４】　第１のプロセスから第２のプロセスへの情報をプロキシサーバによりフィルタリングするデータ処理システムにおいて、該システムは、

中央処理装置と、

オペレーティングシステムと、

命令を格納したメモリとを備え、該命令は、実行されると、

Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）をフィルタ規則として定義し、対応するフィルタサーブレットを定義する工程と、

前記第１のプロセスから前記情報を受け取る工程とを実行し、前記情報はＵＲＬを含み、前記命令は、更に、

前記情報に含まれる前記ＵＲＬが、前記フィルタ規則に含まれる前記ＵＲＬに合致する場合に、前記情報に適用するための、前記定義されたＵＲＬに対応する前記フィルタサーブレットを選択する工程と、

前記フィルタサーブレットに含まれる命令に基づき前記情報を修正することにより、前記フィルタサーブレットを前記情報に適用する工程と、

前記修正された情報を前記第２のプロセスに送信する工程とを実行する。

【請求項２５】　方法を実行するための、第１のプロセスから第２のプロセスへの情報をフィルタリングするためのコンピュータにより実行可能な命令を含むコンピュータ可読媒体であって、該方法は、

前記第１のプロセスから前記情報を受け取る工程と、

前記第１のプロセスにより受け取った情報に適用するためのフィルタを選択す

る工程と、

前記フィルタに含まれる命令に基づき前記情報を修正することにより、前記フィルタを前記情報に適用する工程と、

前記修正された情報を前記第２のプロセスに送信する工程とを備える。

【請求項２６】　第１のプロセスから第２のプロセスへの情報をフィルタリングする方法において、該方法は、

前記第１のプロセスから前記情報を受け取る手段と、

前記第１のプロセスにより受け取った情報に適用するためのフィルタを選択する手段と、

前記フィルタに含まれる命令に基づき前記情報を修正することにより、前記フィルタを前記情報に適用する手段と、

前記修正された情報を前記第２のプロセスに送信する手段とを備える。

【発明の詳細な説明】

【０００１】

（関連出願）

本出願は、１９９８年６月１９日出願の米国仮出願番号６０／０８９，９９５に基づく優先権を主張する。

【０００２】

（発明の技術分野）

本発明は、クライアントプロセスとサーバプロセスとの間で送信される情報のフィルタリングに関し、更に詳しくは、プロキシサーバとプラグインフィルタを用いた、クライアントプロセスとウェブサーバとの間で送信される情報のフィルタリングに関する。

【０００３】

（発明の背景技術）

インターネットの急速な普及により、企業や消費者からアクセス可能な情報量が著しく増加した。情報の流入を管理することが次第に重要度を増している。なぜならば、情報の中には、ユーザがインターネット上で他者に公開されることを望まない、或いは、他者から送られてくることを望まない情報が含まれているからである。コンピュータ或いはネットワークをインターネットに接続することにより、ユーザは、政府機関の情報といった安全な情報から娯楽に関する情報まであらゆるタイプの情報を検索、アクセス及びダウンロードすることができる。インターネットに対する規制は殆ど行われていないこともあり、あらゆるタイプの情報に対するアクセスが劇的に増加した。しかしながら、ユーザがネットワークから取り出す情報に対しフィルタリングを行うことを必要とする場合がある。例えば、企業や政府機関は、セキュリティ情報や機密情報が、例えばローカルネットワーク等の自らのドメインから流出しないようにする必要がある。また、インターネットから受け取る情報は、受け取り側のフォーマットでは操作できないこともあり得る。例えば、インターネットから受け取ったドキュメントの表示解像度の特性は、ドキュメントの受け取り側のユーザがサポートする特性とは異なる可能性がある。

【０００４】

上述の問題に対処するために、ある情報がドメインに流入したり、ドメインから流出したりすることを防ぐシステムが開発されてきた。この様なシステムは、情報のフィルタリングは行うことができるものの、複雑であり、特定の企業に適合させることが容易でない。一般に、情報のフィルタリングを行うシステムは、一旦ソフトウェア開発者により作成されると、どんな情報をどのように除去するかという点をその後変更することは不可能であり、そのためにはソフトウェア開発者が全く新規にフィルタリングシステムを作成し直す必要があった。かかるアプローチにおける問題は、どの情報をどのようにフィルタリングするかというニーズは殆どの場合それぞれの企業及びユーザに特定であり且つ変化するという点にある。異なる内容のフィルタリングをユーザが行おうとする度に、ソフトウェア開発者によりシステムの再構築を行うことは現実的でない。更に、現時点では、最初に受け取った段階でユーザ環境において操作不可能であったデータを、操作可能なように修正するシステムは存在しない。

【０００５】

インターネット、特にワールドワイドウェブ（「ウェブ」）を用いることにより、コンピュータとのインターフェースをとるための機能は簡略化される。ウェブのアーキテクチャは、従来のクライアントサーバモデルに従うものとする。「クライアント」及び「サーバ」という用語は、コンピュータの役割の内、概ねデータの要求者（クライアント）としての役割、或いは、概ねデータの供給者（サーバ）としての役割を表すために用いている。ウェブ環境においては、ウェブブラウザはクライアント側にあり、特定のフォーマットを施された「ウェブドキュメント」はインターネットウェブサーバ側にある。ウェブクライアントとウェブサーバとは、通常、「ｈｙｐｅｒｔｅｘｔ　ｔｒａｎｓｆｅｒｒｅｄ　ｐｒｏｔｏｃｏｌ」（ＨＴＴＰ）と呼ばれるプロトコルを用いて互いに通信を行う。

【０００６】

実行時には、ブラウザがサーバとの接続を開き、ドキュメントに対する要求を行う。サーバは要求されたドキュメントを、通常、標準「ｈｙｐｅｒｔｅｘｔ　ｍａｒｋｕｐ　ｌａｎｇｕａｇｅ」（ＨＴＭＬ）フォーマットで符号化した形式

で引き渡す。ドキュメントを引き渡した後、接続を閉じる。ブラウザはドキュメントを表示し、表示したドキュメントにより指定された機能を実行する。

従って、情報のフィルタリング技術の向上が望まれる。

【０００７】

（発明の概略）

本発明に係る方法、システム、及び製造物は、クライアントプロセスとサーバプロセス間の情報のフィルタリングを行うための既存の情報システムが抱える欠点を、プラグインフィルタを具備するプロキシサーバを備えることにより克服する。プラグインフィルタを具備するプロキシサーバによれば、どの情報をどのようにフィルタリングするかを容易に変更できる。加えて、プラグインフィルタを用いることにより、情報の内容除去のような修正だけでなく、情報の特性をクライアントプロセス或いはサーバプロセスの環境に対応するように修正することも可能になる。

【０００８】

本発明の第１の特徴によれば、ここに具現化しその概要を説明する通り、第１のプロセスから第２のプロセスへの情報をフィルタリングする方法において、該方法は、前記第１のプロセスから前記情報を受け取る工程と、前記第１のプロセスにより受け取った情報に適用するためのフィルタを選択する工程と、前記フィルタに含まれる命令に基づき前記情報を修正することにより、前記フィルタを前記情報に適用する工程と、前記修正された情報を前記第２のプロセスに送信する工程とを備えることを要旨とするものである。前記第１のプロセスはクライアントプロセスであり、前記情報は要求であり、前記第２のプロセスはサーバプロセスであってもよい。前記要求に含まれる前記情報は、セキュリティデータであってもよい。或いは、前記第１のプロセスはサーバプロセスであり、前記第２のプロセスはクライアントプロセスであり、前記情報は応答であり、前記修正された情報は修正された応答であってもよい。更に、前記フィルタリングされた応答をキャッシュメモリに格納してもよい。前記情報に適用するフィルタを選択する前記の工程は、Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）と対応するフィルタとを定義する工程と、前記情報からＵＲＬを取り出す工程と、前

記定義されたＵＲＬが前記取り出されたＵＲＬに合致した場合に、前記情報に適用するための、前記定義されたＵＲＬに対応する前記フィルタを選択する工程とを備えてもよい。

【０００９】

更に、本発明の他の特徴によれば、ここに具現化しその概要を説明する通り、プロキシサーバを使って情報をフィルタリングする方法において、該方法は、クライアントプロセスから要求を受け取る工程と、前記要求に順方向フィルタを適用する工程と、前記フィルタリングされた要求をサーバプロセスに送信する工程と、前記フィルタリングされた要求に関する応答を前記サーバプロセスから受け取る工程と、前記応答に逆方向フィルタを適用する工程と、前記フィルタリングされた応答を前記クライアントに送信する工程とを備えることを要旨とするものである。前記第２のプロセスはウェブサーバであってもよく、この場合、前記順方向フィルタを適用する前記の工程は、ＵＲＬと対応するフィルタとを定義する工程と、前記定義されたＵＲＬが前記要求に含まれている場合に、前記対応するフィルタを使って前記要求をフィルタリングする工程とを含んでもよい。また、前記第２のプロセスがウェブサーバである場合、前記逆方向フィルタを適用する前記の工程は、ＵＲＬと対応するフィルタとを定義する工程と、前記定義されたＵＲＬが前記応答に含まれている場合に、前記対応するフィルタを使って前記要求をフィルタリングする工程とを含んでもよい。前記フィルタリングされた応答をキャッシュメモリに格納してもよい。

【００１０】

更に、本発明の他の特徴によれば、ここに具現化しその概要を説明する通り、プロキシサーバにフィルタを追加する方法において、該方法は、フィルタを受け取るように動作する前記プロキシサーバを作成する工程と、フィルタ規則とフィルタサーブレットとを具備するフィルタを作成する工程と、前記フィルタを前記プロキシサーバに追加する工程とを備え、前記プロキシサーバは、前記追加されたフィルタを使って情報を修正するように動作することを要旨とするものである。複数のフィルタを前記プロキシサーバに追加してもよい。

【００１１】

（発明の詳細な説明）

本明細書に援用され本明細書の一部を構成する添付図面は、本発明の実施を図示し、本発明の詳細な説明と共に本発明の利点と原理を説明するものである。

【００１２】

以下、添付図面に示す本発明の一実施の形態について詳細に説明する。尚、図面及び下記の説明において、同一或いは類似の部分については同一の符号を用いて参照した。

【００１３】

（導入）

本発明に係るシステム及び方法は、クライアントプロセスとサーバプロセス間で送信される情報に対しプラグインフィルタを用いて順方向フィルタリング及び逆方向フィルタリングを行う。プロキシサーバは、サーバプロセスとクライアントプロセスとのインターフェースをとるとともに、両者の間で送信される要求及び応答を監視する。本実施形態において説明するシステム及び方法は、ユーザがフィルタを作成しこれをプロキシサーバに定義することを可能にし、よってユーザはどの情報をどのようにフィルタリングするかを自らのニーズに適合させることができる。これらのプラグインフィルタは、クライアントプロセスとサーバプロセス間の情報をある一定の方法で修正する。この修正は、例えばセキュリティ情報を除去するというような内容を基準とした修正でもよいし、或いは、例えば、表示解像度特性の変更など、サーバプロセスから送られる情報を情報をクライアントプロセスでも操作可能にし互換性を持たせるような変更でも良い。

【００１４】

更に、詳細には、プロキシサーバは、クライアントプロセス及びサーバプロセスとインターフェースされる。フィルタが作成され、プロキシサーバにプラグインされる。フィルタは、フィルタ規則及びフィルタサーブレットを有する。フィルタ規則は、除去すべき情報を規定する。例えば、要求のＵｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ（ＵＲＬ）をフィルタ規則として定義することができ、従って、クライアントプロセスが定義されたＵＲＬへ要求する情報は全て、適用されるフィルタを有することになる。フィルタサーブレットは、実行され

ると要求或いは応答に含まれる情報を修正する実際の命令である。従って、前述の例について述べると、フィルタリングを要する旨を表す標識が一旦要求に付されると、定義されたＵＲＬと突き合わせることによりフィルタ規則に対応するフィルタサーブレットが実行され、要求に含まれる情報を一定の方法で修正する。

【００１５】

本発明に係る方法及びシステムは、また、複数のプラグインフィルタの追加をサポートする。フィルタを追加することにより、ユーザはどの情報をどのように修正するについて多数の変更を行うことができる。更に、かかる方法及びシステムは、クライアントプロセスとサーバプロセス間での要求及び応答の送信に関わる管理タスクを行うように構成することも可能である。また、キャッシュメモリへの格納も実行でき、これにより同一の情報に対する多数のアクセスを速やかに行うことができる。キャッシュメモリへの格納を行う際は、サーバプロセスから受け取った応答に再度フィルタを適用する必要を無くすために、フィルタリングされた応答をキャッシュメモリに格納することが好ましい。

【００１６】

図１は、更に詳細に、ネットワーク１００を介して相互接続されたクライアントサーバシステムの例を示す。この例では、遠隔のサーバシステム１２２はネットワーク１００を介してクライアントシステム１２０に相互接続される。クライアントシステム１２０は、通常の構成要素を含む。例えば、プロセッサ１２４と、メモリ１２５（例えば、ＲＡＭ）と、プロセッサ１２４とメモリ１２５とを接続するバス１２６と、Ｉ／Ｏ制御装置１２８を介してプロセッサ１２４及びメモリ１２５に接続される大容量記憶装置１２７（例えば、磁気ハードディスク、又は、光記憶ディスク）と、通常のモデムのようなネットワークインターフェイス１２９とを含む。

【００１７】

サーバシステム１２２も、通常の構成要素を含む。例えば、プロセッサ１３４と、メモリ１３５（例えば、ＲＡＭ）と、プロセッサ１３４とメモリ１３５とを接続するバス１３６と、Ｉ／Ｏ制御装置１３８を介してプロセッサ１３４及びメモリ１３５に接続される大容量記憶装置１３７（例えば、磁気ディスク又は光デ

ィスク）と、通常のモデムのようなネットワークインターフェイス１３９とを含む。本発明は、クライアントサーバシステム上の大容量記憶装置１２７及び１３７の夫々又はメモリ１２５及び１３５の夫々のようなコンピュータ可読媒体に、実行可能な命令として格納されているソフトウェアにおいて実装されてもよいことが、下記の記載から認識されるであろう。

【００１８】

図１に示されるネットワークは、一例としてのネットワークを示しているが、様々なコンピュータシステムや単一のコンピュータストラクチャにおけるモジュールが情報を交換することを可能にするインターネット、私的ネットワーク及び内部コンピュータストラクチュアを含む如何なるトポロジであっても構わないことが、当業者に理解されるであろう。

【００１９】

図２は、本発明に係る方法及びシステムの実施に好適なデータ処理システムを示す。データ処理システム２００は、イントラネット２０２及びインターネット２０４を有する。イントラネット２０２は、組織のネットワークを表わし、コンピュータ２０６、コンピュータ２０８及びファイアウォール２１４を含む。ファイアウォール２１４はイントラネット２０２への内向トラフィック及びインターネット２０４への外向トラフィックの両方を監視する。コンピュータ２０６とコンピュータ２０８は、どちらも多数の構成要素を有しており、該構成要素には、メモリ２１５、２１７、二次記憶装置２１９、２２１、少なくとも１つのＩ／Ｏ装置２２３、２２５及びプロセッサ２２７、２２９が該当する。インターネット２０４は、コンピュータ２０６及び２０８と同様の構成要素を有するコンピュータ２１０、２１２を含む。イントラネット２０２及びインターネット２０４は２つのコンピュータのみを有するように描写されているが、当業者はこれらのネットワークは、更に多くのコンピュータを含んでもよいことを理解するであろう。加えて、本発明に係る方法及びシステムは他のローカルエリアネットワーク又はワイドエリアネットワークで使用することが可能であることを、当業者は理解するであろう。また、コンピュータ２０６、２０８、２１０、２１２は、更なる構成要素或いは異なる構成要素を含んでもよい。

【００２０】

ファイアウォール２１４はメモリ２２４、プロセッサ２２６及び二次記憶装置２４０を含んでいる。本発明に係る方法及びシステムによれば、メモリ２２４は、プロキシサーバ２２８及びプロキシサーバ２３０を有している。プロキシサーバ２２８及び２３０は、夫々フィルタ２３２、２３４を有している。フィルタ２３２を用いて、プロキシサーバ２２８は、「順方向フィルタリング」を実行する。「順方向フィルタリング」は、プロキシサーバが、イントラネット２０２内部から発生するとともにインターネット２０４へ送られる要求に対してだけでなく、これらの要求の応答に対して行うフィルタリングを表わす。例えば、コンピュータ２０６のクライアントプログラム２１６は、コンピュータ２１０のサーバプログラム２２０にアクセスしようとする。この場合には、フィルタ２３２は、ブロックされるべき求及び応答の全ての部分だけでなく、ファイアウォールを通過して流れることができる外向要求及び内向応答をも表わす。即ち、本発明に係る方法及びシステムによって実行されるフィルタリングは、ウェブサイトの一部がアクセスされることをブロックすること、又は、ウェブサイト全体がアクセスされることをブロックすることを含む。

【００２１】

フィルタ２３４を用いて、プロキシサーバ２３０は、「逆方向フィルタリング」を実行する。「逆方向フィルタリング」は、プロキシサーバが、インターネット２０４から発生するとともにイントラネット２０２へ送られる要求に対してだけでなく、これらの要求の応答に対して行うフィルタリングを表す。例えば、コンピュータ２１２のクライアントプログラム２２２は、コンピュータ２０８のサーバプログラム２１８にアクセスしようとする。この場合には、プロキシサーバ２３０は、フィルタ２３４を用いて、どの要求及び応答がエンティティ内に入ってくることができるか、どの要求及び応答が修正しなければエンティティ内に入ってこれないかを決定する。

【００２２】

プロキシサーバは、フィルタ２３２、２３４に加えて、プロキシサーバはサーブレット２３６、２３８を含んでいる。このサーブレット２３６、２３８は、プ

ロキシサーバが、例えば、ｈｙｐｅｒｔｅｘｔ ｔｒａｎｓｆｅｒ ｐｒｏｔｏｃｏｌ（ＨＴＴＰ）など、多数ある周知のプロトコルのいずれかを使って通信を行うことを可能にするコードである。本発明に係る方法及びシステムによれば、単一のプロキシサーバを順方向フィルタリングと逆方向フィルタリングとの両方を実行するように構成することが可能である。また、プロキシサーバは、ファイアウォール２１４以外にも、コンピュータなどの他の装置上に配置することも可能である。尚、本発明の実施態様例はメモリに格納するものとして説明したが、かかる実施態様例は、ハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ、インターネットなどのネットワークからの搬送波、或いは他の形態のＲＡＭ若しくはＲＯＭに格納し、そこから読み出すようにすることが可能であることを、当業者は理解するであろう。

【００２３】

本発明に係る方法及びシステムに従ったプロキシサーバの他の特徴は、かかるプロキシサーバは、要求に応じて遠隔位置からデータを取り出した後、ファイアウォール２１４のキャッシュ２４２にこのデータを格納するという点にある。これにより、このデータの要求はこれ以降全て、通信オーバーヘッドを伴うことなくなく、ローカルな記憶場所に格納されたコピーを用いて実行することが可能である。キャッシュメモリに格納されたデータは、フィルタリングされたバージョンとなる。従って、フィルタ（例えば、フィルタ２３４）がデータから内容を取り除く場合、この修正されたバージョンがキャッシュメモリに格納されることになる。このデータはプロトコルに依存することなしにキャッシュメモリに格納される。即ち、データのアクセスに使用されるプロトコル（例えば、ＨＴＴＰやＦＴＰ）に関わらず、データはキャッシュ２４２に格納される。従って、キャッシュ２４２は、異なるプロトコルを用いてアクセスされたデータを含み得る。本発明に係る方法及びシステムは、データを二次記憶装置に格納するものとして説明したが、或いは、他の実施形態としてデータをメモリ２２４に格納してもよい。

【００２４】

図３は、本発明の例示的実施形態に従った、情報のフィルタリングに用いられるプロキシサーバアーキテクチャを示した図である。本発明の一実施形態におい

て、プロキシサーバ３００の構成要素には、フィルタ規則を含んだ要求フィルタ３１０、同じくフィルタ規則を含んだ応答フィルタ３２０、及び、プロキシサーバプロセッシング構成要素３１５が含まれる。プロキシサーバは、サーバプロセス３２５からの情報を要求するクライアントプロセス３０５とのインターフェースをとる。クライアントは、ネットワークに接続されたコンピュータ、或いは、サーバ３２５に直接に接続されたコンピュータなど、どのコンピュータであってもい。通常、クライアントはサーバに送る要求を生成するとともにこの要求を満たす応答をサーバから受け取る。

【００２５】

プロキシサーバ３００は、論理上はクライアントプロセス３０５とサーバプロセス３２５との間に位置し、企業のファイアウォール内に組み込むことも可能である。プロキシサーバ内では、要求フィルタ３１０は、クライアントによって送られるサーバ情報を求める要求を受け取る。要求フィルタ３１０は、受け取った要求を分析し、要求の中に、プロキシサーバプロセッシング領域３１５において定義されるフィルタの対象となる情報が含まれているかを決定する。この分析はフィルタ規則を用いて実行される。フィルタ規則はフィルタリングすべき情報を定義する。一実施形態では、フィルタ規則は、Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ（ＵＲＬ）を含んでおり、従って、要求を受け取ると、ＵＲＬをフィルタ規則に照らして検査し、かかる要求がフィルタリングすべき情報であるかどうかを検査する。ＵＲＬの検査は、当業者に周知のどの方法でも行うことができる。例えば、フィルタ規則をテーブルに納める方法、データベースによる方法、或いは、正則表現を生成して、ＵＲＬと生成した正則表現とを比較する方法などである。

【００２６】

要求に対しフィルタリングを行う必要がある場合、即ち、フィルタ規則のいずれかが満たされた場合は、かかる要求はプロキシサーバプロセッシング３１５に引き渡され、要求に含まれる情報の内フィルタサーブレットにより定義される情報を修正する。フィルタサーブレットは、実行されると要求に対する修正を行う命令を含んでいる。要求をサーバプロセスに送信するに先立ち、かかる要求から

全てのセキュリティ情報を除去するようプロキシサーバに命令するのは、例えば、このサーブレットである。

【００２７】

サーバは、クライアント３０５に送り返すための、要求に対する応答を生成する。本発明の一実施形態では、応答はクライアントに直接は送られず、プロキシサーバ３００に送られ、応答フィルタ３２０がこれを受け取る。要求フィルタ規則の場合と同様に、応答フィルタ規則は応答を検査し、かかる応答はクライアントプロセスへの送信に先立ちフィルタリングを行う必要があるかどうかを決定する。応答はフィルタリングされて、問題のありそうな情報が除去されてクライアントに渡されないようになったり、或いは、情報がクライアント側の環境で機能するように修正されたりする。例えば、サーバプロセスにより定義されているが、クライアントプロセスとは互換性がない表示解像度の修正が行われる。

【００２８】

応答が応答フィルタ規則のいずれかを満たす場合、プロキシサーバは、フィルタサーブレットの内の満たされたフィルタ規則に対応するものを前記応答に適用する。プロキシサーバは、要求フィルタリングと応答フィルタリングとの両方を同時に実行する必要がないことは、当業者には理解されよう。プロキシサーバは要求のみ、或いは、応答のみを処理すればよい。どの情報をどのようにフィルタリングするかは、ユーザにより定義される。

【００２９】

プロキシサーバプロセッシング構成要素３１５は、プロキシサーバ３００に対して定義付けされたいずれかのフィルタの規定に従って情報を修正する。これらのフィルタ、即ちフィルタ規則及びサーブレットは、モジュールになっており、要求フィルタ規則或いは応答フィルタ規則を定義するとともにこれを適切な規則構成要素に対し定義付けすることにより、プロキシサーバに差し込むことが可能である。これにより、フィルタ規則に対応するフィルタサーブレットが、プロキシサーバプロセッシング構成要素に対し定義付けされる。

【００３０】

プロキシサーバプロセッシングは、フィルタサーブレットの適用に加え、他の

機能も実行する。ここで言う他の機能とは、応答及び要求のログを記録する機能や、サーバプロセスにより受け取ったフィルタリング後の応答をキャッシュに格納して速やかに取り出せるようにする機能を含む。キャッシュへ格納することにより、他のクライアントが同じ情報を要求した場合、サーバプロセスに新たに要求を送る代わりに、かかる情報をキャッシュから取り出すことができるので、取り出しに要する時間を短縮できるという利点が得られる。応答をキャッシュに格納する場合、フィルタリングを行った後の応答を格納することが好ましい。フィルタリングされた応答をキャッシュに格納することにより、キャッシュから応答を取り出した場合でも、プロキシサーバに応答を再びフィルタリングさせることを防ぐことができる。

【００３１】

図３には、１つのクライアントプロセスと、１つのサーバプロセスと、１つのプロキシサーバを図示したが、１つのプロキシサーバに接続されたクライアントプロセスが複数あってもよいし、クライアントプロセス及びサーバプロセスからの要求及び応答のフィルタリングを行うように連鎖されたプロキシサーバが複数あってもよいことは、当業者には理解されるであろう。加えて、クライアントプロセスがネットワークを介してアクセスするサーバプロセスが複数あっても良い。また、図３にはネットワークを示していないが、本発明は、クライアントからサーバに送られる情報、或いは逆にサーバからクライアントに送られる情報、のプロキシサーバによる処理にその重点を置くことが当業者には理解されよう。ネットワークは、クライアントプロセスとプロキシサーバとの間、プロキシサーバとサーバプロセスとの間、或いは、クライアントプロセスとサーバプロセスとの間であればどこに位置してもよい。

【００３２】

図４は、順方向フィルタリングと逆方向フィルタリングにおいて実行される主なステップを示したフローチャートである。順方向フィルタリングは、上述したように、クライアントプロセスからの外向要求に対して実行されるフィルタリングと定義される。これとは逆に、逆方向フィルタリングは、サーバプロセスからクライアントプロセスへ向けた内向応答に対して実行されるフィルタリングと定

義される。この処理は、サーバプロセスの情報に対する要求をクライアントプロセスから受け取ると開始される（ステップ４００）。本発明の一実施形態において、サーバプロセスはウェブサーバであり、クライアントプロセスは、インターネットに接続されており、ウェブブラウザを用いて情報へのアクセスを行うコンピュータである。

【００３３】

要求の受取に続き、本発明に係るシステム及び方法は、その要求に対し順方向フィルタを適用する（ステップ４０５）。順方向フィルタは、例えば、企業が該企業のドメイン外に流出することを望まないセキュリティ情報を全て取り除くこともできる。要求の受け取りに応じて、サーバプロセスは、クライアントプロセスに送り返すための、要求に対する応答を生成する。応答には、例えば、クライアントプロセスにより要求されたウェブサーバのドキュメントが含まれる。この後、プロキシサーバは前記要求を満たすこの応答を受け取る（ステップ４１０）。

【００３４】

一実施形態では、応答は以前にサーバから受け取られ、プロキシサーバからアクセス可能であるキャッシュに格納されている。応答がキャッシュに格納されると、かかる応答は、サーバプロセスに対し新たな要求を行うことなしに直接クライアントプロセスに送られるので、応答の取り出しに要する時間を短縮できる。この際、キャッシュに格納された古い応答をクライアントに送ることを防ぐため、タイムスタンプを用いることが望ましい。タイムスタンプは、無効になったものの依然としてキャッシュに残っている古いデータを除去する処理として当業者には周知である。更に、キャッシュへの格納に先立ち応答をフィルタリングすることが望ましい。これにより、プロキシサーバが再びフィルタリング処理を行うことなく、フィルタリングされた応答を直接クライアントプロセスに送ることが可能になる。

【００３５】

応答がキャッシュに格納されていない場合は、本発明に係るシステム及び方法は、サーバプロセスから応答を受け取った後、受け取った応答に逆方向フィルタ

リングを適用する（ステップ４１５）。順方向フィルタリングの場合と同様に、逆方向フィルタリングも応答に含まれる情報の修正を行う。逆方向フィルタリングの例として、クライアントプロセスの環境において情報が機能するようにパラメータを修正すること、問題のありそうな情報を除去することが挙げられる。

【００３６】

逆方向フィルタリングの適用に続き、フィルタリングされた応答はそれぞれの用途のためにクライアントに送られる（ステップ４２０）。フィルタリングされた応答は、フィルタによる定義に従って情報の除去、修正を行っており、プロキシサーバを含むドメインの要求を満たしていることになる。応答をクライアントプロセスへ送信後、プロキシサーバは、フィルタリングされた応答の「後処理」を行ってもよい（ステップ４２５）。プロキシサーバがフィルタリングされた応答をキャッシュに格納するのは、例えばこの段階で行ってもよい。加えて、例えば、プロキシサーバを通過した要求及び応答のログを記録するなどの他の管理用の機能もこの段階で実行してもよい。

【００３７】

図５は、本発明の例示的実施形態に従った様式で、要求或いは応答のフィルタリングを行うためのステップを示したフローチャートである。図５には、図４において大まかに示したステップ４０５及びステップ４１５の更に詳細なステップを示す。要求或いは応答を受け取ると、本発明に係るシステム及び方法は、これに引き続き要求或いは応答中のＵＲＬ又はドメインを識別する（ステップ５０５）。本発明の一実施形態においては、クライアントは、ウェブサーバに要求を出し、これに応えウェブサーバは応答を送る。この要求と応答とは、夫々クライアントプロセスとサーバプロセスのＵＲＬをそれぞれ表示している。本発明に係るシステム及び方法は、この情報を使ってかかる要求又は応答がフィルタリングすべきものであるかどうかを決定する。従って、本発明に係るシステム及び方法は、応答或いは要求に含まれるＵＲＬの識別に引き続き、識別されたＵＲＬに対するフィルタが存在するかどうかを決定する（ステップ５１０）。

【００３８】

フィルタが作成されプロキシサーバに追加されると（図６を参照して更に詳細

に後述する）、プロキシサーバは、要求或いは応答に対しフィルタリングすべき、又は、フィルタを適用すべきＵＲＬを識別するフィルタ規則を与えられる。このＵＲＬのリストは、探索機能を実行するのに用いることができるものであれば、テーブル、データベース、或いは他のどのようなデータ構造であってもよい。本発明に係るシステム及び方法が、要求或いは応答を受け取ると、サーバプロセスのＵＲＬ情報が検出される。このＵＲＬ情報を使って、本発明に係るシステム及び方法は、ＵＲＬ情報をプロキシサーバに対し定義付けされた全てのフィルタ規則と比較する。

【００３９】

ＵＲＬ情報をフィルタ規則と比較し、かかる応答或いは要求に対応するフィルタがあると判定すると、本発明に係るシステム及び方法は、フィルタ規則に対応するフィルタサーブレットの命令による定義通りに、応答或いは要求に対しフィルタを適用する（ステップ５１５）。これらの命令は、実行されると、要求或いは応答をフィルタサーブレットに規定されたように修正する。応答或いは要求に対してフィルタが適用されると、フィルタリングされた情報は、応答であればクライアントに、要求であればサーバに渡される（ステップ５２０）。

【００４０】

図６は、本発明の例示的な一実施形態に従った様式で、プロキシサーバにフィルタを追加するのに必要なステップを示したフローチャートである。本発明の利点の１つは、全く新しいソフトウェアをプロキシサーバ用に開発することなしに、種々のフィルタをプロキシサーバに「プラグイン（差し込み）」することができるという点にある。これにより、ローカルのシステムの管理者が、或るドメインに特有の所望の情報をフィルタリングするように、プロキシサーバを調整することが可能になる。本発明に係るシステム及び方法は、フィルタサーブレットを作成することによりプロキシサーバにフィルタを追加することができる（ステップ６００）。サーブレットとは、フィルタ規則に対応付けられているとともに、実行されると、システム管理者の要件を満たすように要求或いは応答を修正する一連の命令である。

【００４１】

次に、フィルタ規則が作成され（ステップ６０５）、これをきっかけとしてフィルタサーブレットが実行される。フィルタ規則は、ステップ６００においてフィルタサーブレット内に作成した命令を適用すべきドメインの識別子であり、例えばＵＲＬである。例えば、ユーザは、セキュリティの観点から特に関心のある多数のウェブアドレス或いはＵＲＬを、プロキシサーバに対するフィルタ規則として指定することができる。ＵＲＬを含む要求或いは応答をプロキシサーバにより受け取ると、受け取ったＵＲＬが予め定義されたフィルタ規則のいずれかに一致するかを決定するためのテストが実行される。一致が見られれば、一致したフィルタ規則に対応するフィルタサーブレットが実行され、要求或いは応答に適用される。

【００４２】

フィルタサーブレット及びフィルタ規則の作成後、本発明に係るシステム及び方法は、プロキシサーバに新たなフィルタ規則を識別させる（ステップ６１０）。システム管理者が自らのドメインに入ってくる情報の保護或いは修正を行うためのフィルタ規則及びフィルタサーブレットを作成する場合には、これらのフィルタは実行可能になるためプロキシサーバに対し明確にされる必要がある。プロキシサーバにフィルタを識別させる際、このフィルタ規則は他のフィルタ規則とともにリストに含めることが望ましい。これは、プロキシサーバが、取り出したＵＲＬをフィルタリングすべき全てのフィルタ規則と比較できるようにするためである。

【００４３】

次に、フィルタ規則は、要求或いは応答のいずれに適用されるかをプロキシサーバに識別される（ステップ６１５）。これにより、プロキシサーバが要求に対してフィルタを適用すべき時に誤って応答に対してフィルタを適用したり、或いはその逆を行ったりすることを防ぐ。

【００４４】

最後に、フィルタサーブレットの位置をプロキシサーバに識別させる（ステップ６２０）。これは、フィルターサブレットを他の全てのフィルタサーブレットと同じ位置に位置させることにより実行できる。全てのフィルタサーブレットを

同一の位置に置くことにより、プロキシサーバが所望のフィルタサーブレットを検索する手間を省くことができる。しかしながら、コードを他のコードと識別するためのソフトウェア設計は多数存在する。例えば、位置情報にポインタを用いた、データベースを維持するソフトウェア設計などである。プロキシサーバにフィルタサーブレットの位置を与えるこの例は、選択肢の１つであり、かかる機能を提供する種々の実施の形態は、本発明の範囲に含まれるものとみなされる。

【００４５】

（結論）

以上説明したように、本発明に従った様式でクライアントプロセスとサーバプロセス間の情報をフィルタリングするシステム及び方法によれば、特定のドメインのニーズを満たすようにフィルタを適合させることが容易に行える。フィルタをプラグイン可能にすることにより、要求及び応答から取り除くべき情報のタイプの情報に加えて、ユーザはフィルタリングすべき情報を容易に且つ動的に修正することが可能である。更に、フィルタリングされた応答をキャッシュに格納することにより、クライアントプロセスが同じ情報を要求した場合の処理時間が大幅に短縮される。

【００４６】

上述の本発明の実施形態についての説明は、あくまでも説明のために提示したものであり、本発明を網羅するものでも、開示した特定の形態に限定するものでもない。上述の教示に照らして或いは本発明の実施を通して、様々な変容、変形が可能である。例えば、上述の説明ではソフトウェアを含む実施形態としたが、本発明に係るシステム及び方法はハードウェアとソフトウェアとの組合せとして、或いは、ハードウェアのみとして実施することが可能である。本発明はオブジェクト指向プログラミング言語、及び、非オブジェクト指向プログラミング言語を用いて実施することが可能である。加えて、本発明の実施態様例はメモリに格納するものとして説明したが、これらの実施態様例は、ハードディスク、フロッピーディスク、或いはＣＤ－ＲＯＭなどの二次記憶装置、インターネットからの搬送波や他の伝播媒体、或いはこれ以外の形態のＲＡＭやＲＯＭなど、メモリ以外のタイプのコンピュータ可読媒体に格納してもよいことは、当業者には理解され

るであろう。本発明の範囲は特許請求の範囲及びその均等物により定義される。

【図面の簡単な説明】

【図１】

クライアントシステムとサーバシステムとを含むコンピュータネットワークを示した図である。

【図２】

本発明に係る方法及びシステムの実施に好適なデータ処理システムを示した図である。

【図３】

本発明の例示的実施形態に従った様式で情報をフィルタリングするのに用いられるプロキシサーバアーキテクチャの構成要素を示した図である。

【図４】

本発明の例示的実施形態に従った様式で情報の順方向フィルタリング及び逆方向フィルタリングを実行する際の主な工程を示したフローチャートである。

【図５】

本発明の例示的実施形態に従った様式で要求或いは応答をフィルタリングするための工程を示したフローチャートである。

【図６】

本発明の例示的実施形態に従った様式でプロキシサーバにフィルタを追加するのに必要な工程を示したフローチャートである。

【符号の説明】

２００	データ処理システム
２０２	イントラネット
２０４	インターネット
２０６、２０８、２１０、２１２	コンピュータ
２１４	ファイアウォール
２１５、２１７、２２４	メモリ
２１６、２２２	クライアントプログラム
２１８、２２０	サーバプログラム

２１９、２２１、２４０	二次記憶装置
２２３、２２５	Ｉ／Ｏ装置
２２６、２２７、２２９	プロセッサ
２２８、２３０	プロキシサーバ
２３２、２３４	フィルタ
２３６、２３８	サーブレット
２４２	キャッシュ
３００	プロキシサーバ
３０５	クライアントプロセス
３１０	要求フィルタ
３１５	プロキシサーバプロセッシング
３２０	応答フィルタ
３２５	サーバプロセス

【図１】

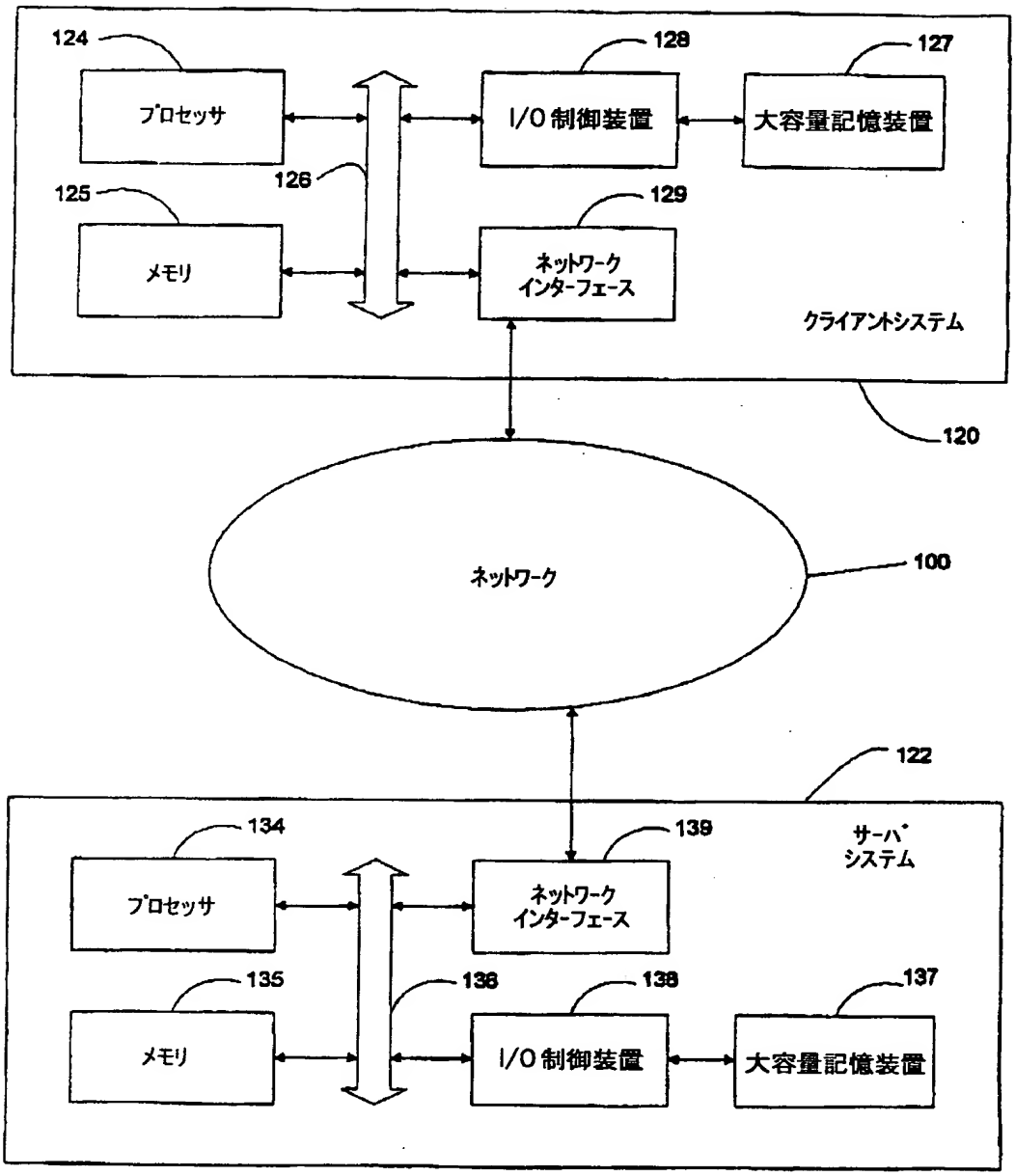

124
プロセッサ
125
メモリ
126
128
I/O制御装置
129
ネットワーク
インターフェース
127
大容量記憶装置
クライアントシステム
120
ネットワーク
100
122
サーバ
システム
134
プロセッサ
135
メモリ
136
139
ネットワーク
インターフェース
138
I/O制御装置
137
大容量記憶装置

FIG. 1

【図２】

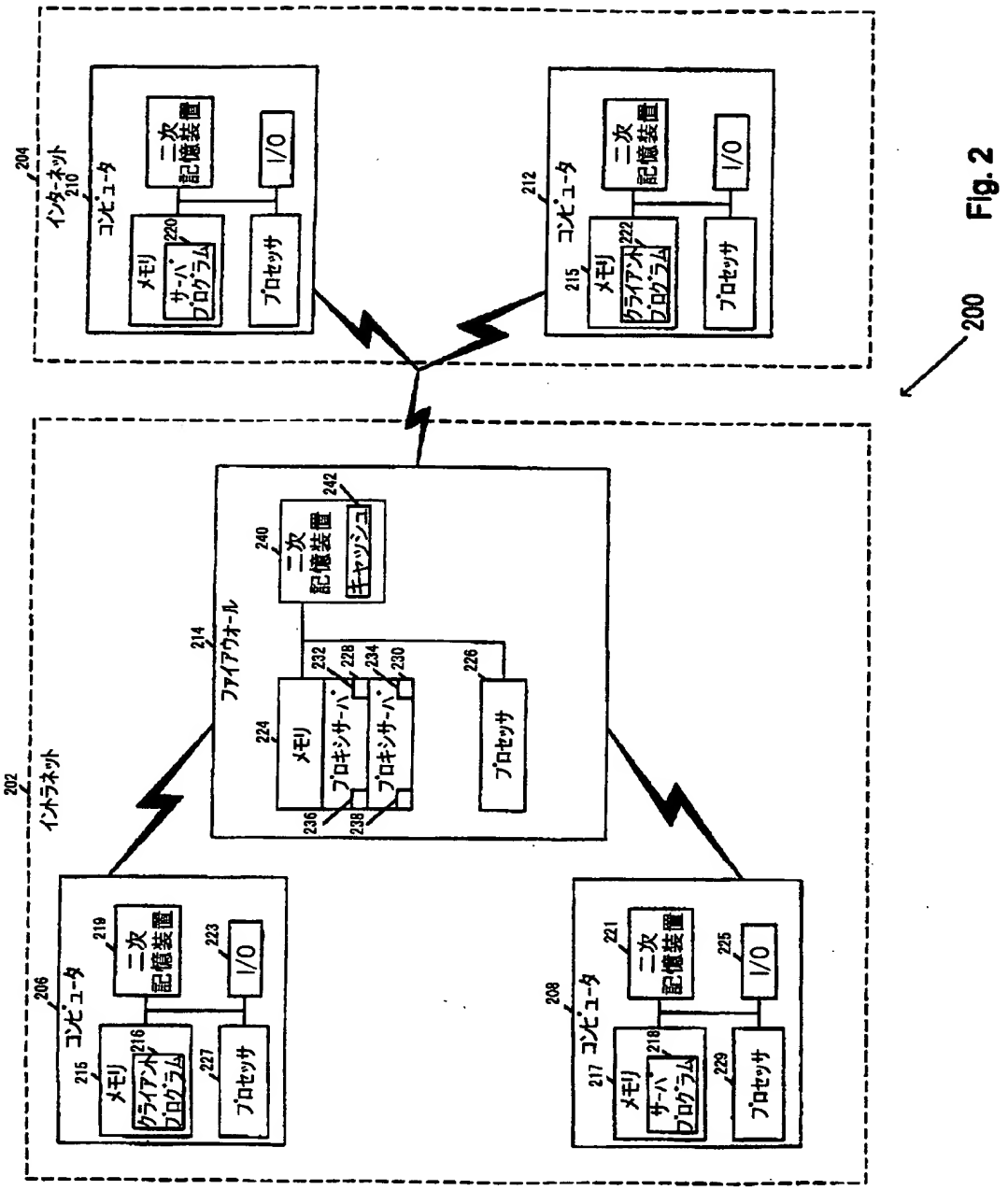

200
204
インターネット
210
コンピュータ
二次記憶装置
I/O
メモリ
サーバプログラム
220
プロセッサ
212
コンピュータ
二次記憶装置
I/O
メモリ
クライアントプログラム
222
215
プロセッサ
202
イントラネット
214
ファイアウォール
240
二次記憶装置
キャッシュ
242
メモリ
232
228
プロキシサーバ
234
プロキシサーバ
230
224
226
プロセッサ
236
238
206
コンピュータ
219
二次記憶装置
223
I/O
メモリ
クライアントプログラム
216
215
227
プロセッサ
208
コンピュータ
221
二次記憶装置
225
I/O
メモリ
サーバプログラム
218
217
229
プロセッサ

Fig. 2

【図３】

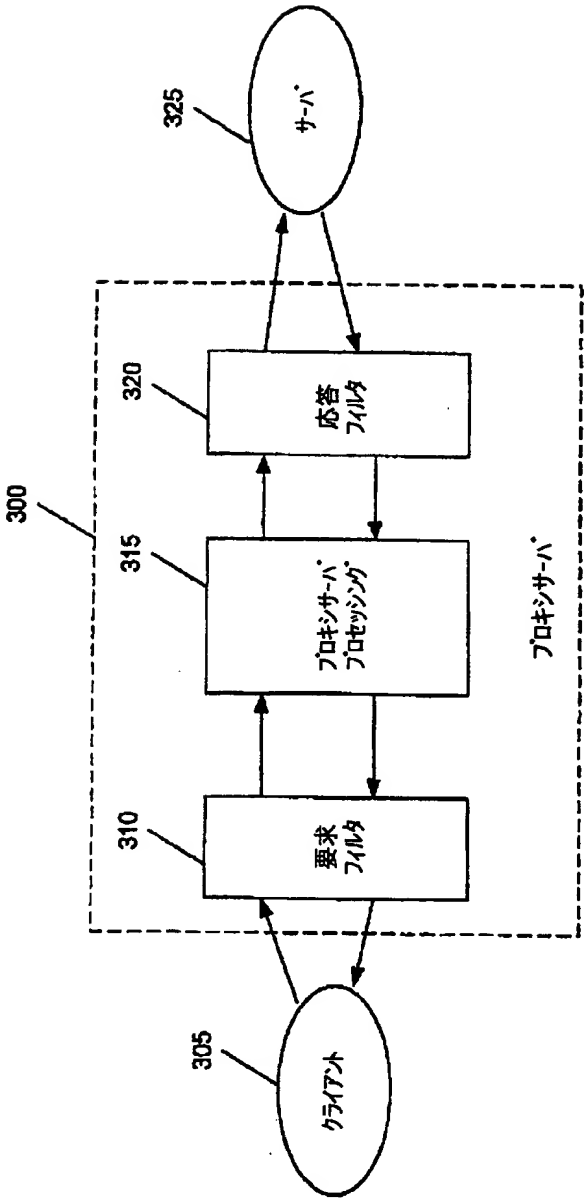

325
サーバ
320
応答
フィルタ
300
315
プロキシサーバ
プロセッシング
プロキシサーバ
310
要求
フィルタ
305
クライアント

Fig. 3

【図４】

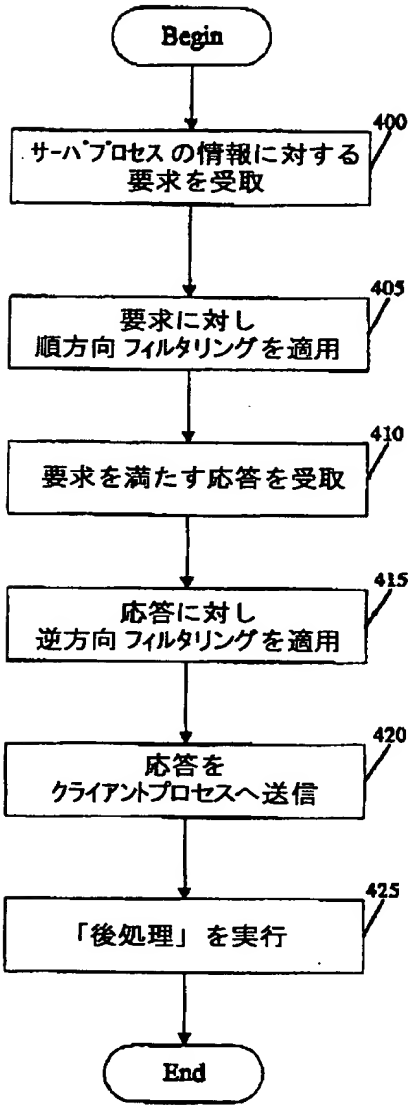

Begin
サーバプロセスの情報に対する要求を受取
400
要求に対し順方向フィルタリングを適用
405
要求を満たす応答を受取
410
応答に対し逆方向フィルタリングを適用
415
応答をクライアントプロセスへ送信
420
「後処理」を実行
425
End

Fig. 4

【図５】

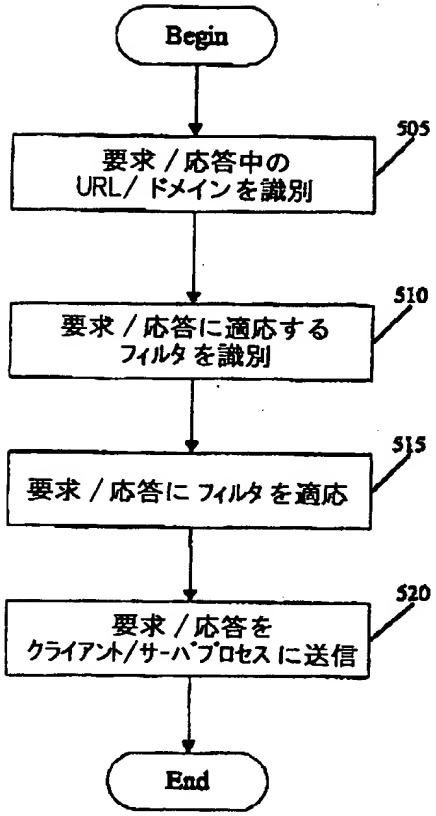

Begin
505
要求／応答中の
URL／ドメインを識別
510
要求／応答に適応する
フィルタを識別
515
要求／応答にフィルタを適応
520
要求／応答を
クライアント/サーバプロセスに送信
End

Fig. 5

【図６】

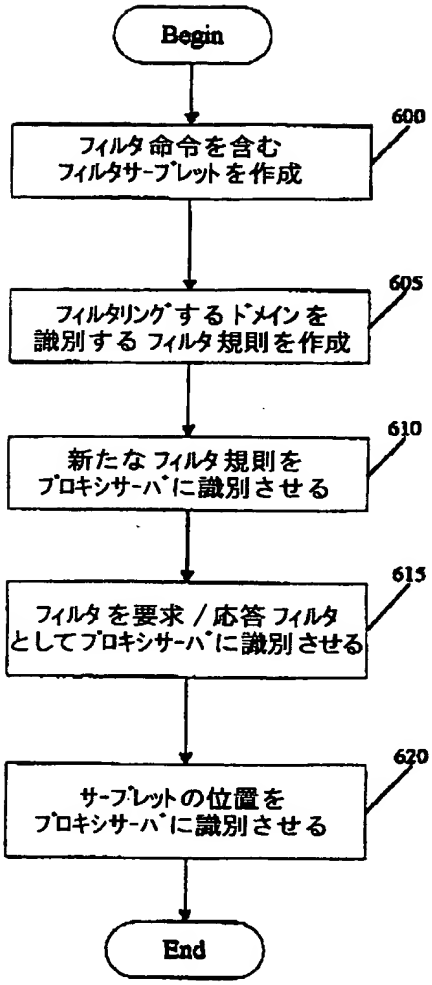

Begin
フィルタ命令を含む
フィルタサーブレットを作成
600
フィルタリングするドメインを
識別するフィルタ規則を作成
605
新たなフィルタ規則を
プロキシサーバに識別させる
610
フィルタを要求／応答フィルタ
としてプロキシサーバに識別させる
615
サーブレットの位置を
プロキシサーバに識別させる
620
End

Fig. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/13876

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06F 12/14, 13/14
US CL :709/225,229; 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/225,229; 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
STN: Compendex, Inspec, Uspatfull
search terms: firewall, proxy, filter, URL, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,805,820 A (BELLOVIN et al) 08 September 1998, col. 4, lines 40-65, col. 9, lines 6-43, col. 7, line 1 - col. 8, line 53.	1-26
Y,P	US 5,835,726 A (SHWED et al) 10 November 1998, col. 5, line 39 - col. 8, line 40, col. 9, line 1 - col. 11, line 13.	1-26
A,P	US 5,884,025 A (BAEHR et al) 16 March 1999, col. 1, line 1 - col. 2, line 49.	1-26
A,P	US 5,864,666 A (SHRADER) 26 January 1999, col. 1, line 6 - col. 2, line 9, col. 8, line 20 - col. 9, line 3.	1-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 13 OCTOBER 1999	Date of mailing of the international search report 07 DEC 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PAUL KANG for Eugene Zoyan Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet)(July 1992) *

フロントページの続き

(72)発明者 シン インダージート
アメリカ合衆国、94040 カリフォルニア
州、マウンテン ビュー、 パーク ドラ
イブ1339 7

Fターム(参考) 5B082 GA02 HA07 HA08
5B089 GA19 GB01 GB03 JA21 KA08
KA10 KA17 KH00